ISSN:0975-9646

An Extended Visual Cryptography Algorithm for Quality-Improved Gray Scale Image with Sigmoid Function.

Santosh Kumar
Dept.of C.S.E
NRIST-Bhopal, India.

Prof. Sini Shibu
Dept.of C.S.E
NRIST-Bhopal, India.

***Abstract*—Conventional visual secret sharing schemes generate noise-like random pixels on shares to hide secret images. It suffers amanagement problem, because of which dealers cannot visually identify each share. This problem is solved by the extended visual cryptography scheme (EVCS), which adds ameaningful cover image in each share. However, the previous approaches involving the EVCS for general access structures suffer from a pixel expansion problem. In addition, the visual cryptography (VC)-based approach needs a sophisticated codebook design for various schemes.**
In this paper, a novel method of VC is presented for halftone images which represent the resultant image in the same size as the original secret image Contrast the visual information based on pseudo randomization and pixel reversal using sigmoid function is also proposed.

***Index Terms*—Extended visual cryptography (EVC), general access structures, pixel expansion, visual secret sharing scems.**

INTRODUCTION:

With the coming era of electronic commerce applications, there is an urgent need to solve the problem of ensuring information safety in today's increasing open network environment. The encrypting technologies of traditional cryptography are usually used to protect information security. With such technologies, the data become disordered after being encrypted and can then be recovered by a correct key, needing a computational overhead in decryption. Without the correct key, the encrypted source content can hardly be detected even though unauthorized persons steal the data.

Naor and Shamir proposed a new concept of visual cryptography (VC) in 1994 [1]. Visual cryptography, an emerging cryptography technology, uses the characteristics of human vision to decrypt encrypted images. It needs neither cryptography knowledge nor complex computation. For security concerns, it also ensures that hackers cannot perceive any clues about a secret image from individual cover images. The basic idea is to partition the data into *n* pieces called the shares. Only when a sufficient number of shares are stacked together will human eyes recognize the image content. According to the basic model proposed by Naor and Shamir, a (2, 2) visual cryptography scheme that encodes a secret image into 2 shares, revealing the secret image by share stacking. The most notable feature of this approach is that it can recover a secret image without any computation. It exploits the human visual system to read the secret message from some overlapping shares, thus overcoming the disadvantage of complex computation required in the traditional cryptography.

The threshold scheme makes the application of visual cryptography more flexible. With the *t* out of *n* threshold scheme *(t < n)*; the manager can first produces n copies of transparency drawn from the secret image, one for each of his members. If any *t* of them stacks their transparencies together, the content of the secret image will show up. If the number of transparencies is less than *t*, the content of the secret image will remain hidden. In this approach, a page of cipher text and a printed transparency serves as a secret key. The original text is revealed through placing transparency with key over the ciphered page though they are indistinguishable from random noise. A secret picture must be shared among n participants. The picture is divided into *n* transparencies so that if m transparencies are placed together the picture is visible. When there are fewer *m* transparencies it is invisible. This ensures that the secret picture is viewed as a set of black and white pixels with each pixel being handled separately.

RESEARCH FINDINGS:

The existing approach generates shares pixels, based on pixel reversal, random reduction in original pixel and subtractions of the original pixel.

The (2, 2) VC scheme existing in the literature divides the secret image into two shares so that reconstruction of an image from a share is impossible. Each share is printed in transparencies.

The original secret image is divided so that it reveals the secret image after OR operation of qualified shares. This approach reveals reduced pixel expansion, required for retrieval of the secret image.

An efficient c-color (k, n)-threshold visual and secret sharing scheme were developed. VC methods where the same technique is used to decompose the color secret image into three separate images that are respectively colored cyan (C), magenta (M) and yellow (Y). Then the halftone technique is used to translate the three color images into halftone images. Finally, by combining the three halftone images, a color halftone image can be generated. Dividing pixels into two or more sub pixel helps secret picture retrieval.

EXISTING APPROACHES:

Naor & Shamir [6] implemented a (2, 2) visual cryptography where decoded image is double than that of the original secret image as pixel p expanded into two sub

pixels. This is called pixel expansion, affecting the contrast of resulting image. The (2, 2) visual cryptography scheme has one secret halftone (gray scale) image (SI) as algorithm input, where SI is said to be a matrix Sij and i and j shows pixel positions and i, j= 1, 2, 3… n.

Input: Secret Gray scale image (SI)
Output: Valid Shares Share1, Share2
Method:
Step1:- Pixel Sij with position i and j is the input called original pixel.
Step2:- Apply pixel reversal i.e Sij´ = 255 – Sij .
Step3:- Use pseudo - random number generator (0.1 to 0.9) to reduce Si j´ randomly.
Step4:- Take the difference of Sij´ with original pixel Sij.
Step5:- Use pseudo-random number generator to reduce reversed value of Sij´ randomly.
Step6:- Apply pixel reversal i.e Sij´´ = 255 – Sij´
Step7:- Store in matrix as image called share 1.
Step8:- Take the difference of two random number generators with original pixel S ij .
Step9:- Apply pixel reversal i.e Sij´´´ = 255 - Sij´.
Step10:- Store Sij´´´ in matrix as **image** called share 2.
Step11:- Repeat point 1 to 10 for all pixels from original image (i.e. matrix of original image)

Here the decoded image and original secret message are of same sizes since there is no pixel expansion effort. But the algorithm is as general as with other decrypted image schemes which are darker, containing much visual impairment. The secret decoded image is darker than the original and increases spatial resolution. The visual cryptography has the same effect in the decoded image

OBJECTIVES:

The overall objective of this work is mentioned below:

- To develop an algorithm that provides secret image that possesses a much higher readability.
- To propose an approach which provides highly effective contrast enhanced secret images.
- To propose an approach that improves details in images without affecting the image or increasing any amount of noise present to the output image. Improve the visibility Factor in the resultant image thus make it easy to take a decision and provide better security.

PROBLEM FORMULATION:

The existing approach generates shares pixels, based on pixel reversal, random reduction in original pixel and subtractions of the original pixel. The original secret image is divided so that it reveals the secret image after OR operation of qualified shares. This approach reveals reduced pixel expansion, required for retrieval of the secret image.
But dividing pixels into two or more sub pixel helps secret picture retrieval with additional impairments and poor resolutions. This approach also results in poor contrast, which degrades the visibility and performance for retrieval of the secret image as the contrast of an image is a very important characteristics by which the image can be judged.

Our proposed methodology overcomes the drawback of the existing approach by applying sigmoid function in spatial domain for contrast improvement in the resulting secret image. To achieve contrast enhancement, a novel mask based on using the input value together with the sigmoid function is passing over the target image, operates on its pixels one by one.
The resulting image possesses a much higher readability and proves highly effective in dealing with poor contrast images. This approach enhances details in images without affecting the details or increasing any amount of noise present to the output image.

THE PROPOSED METHODOLOGY :

The Sigmoid Function is a mathematical function having an "S" shape (sigmoid curve). The sigmoid function refers to the special case of the logistic function defined by the formula

$$S(t) = \frac{1}{1 + e^{-t}}.$$

The proposed approach defines the application of the sigmoid function for the contrast improvement in resulting secret image. The proposed approach deals with a mask based on the input parameter using a non linear activation function i.e. the sigmoid function. The mask is passed over the entire image pixel by pixel and resultant image is the processed image after adjusting and contrast enhancement
In proposed methodology, an extension of secret sharing schemes is visual cryptography that aims at splitting images into two or more shares such that when a predetermined number of shares are aligned and stacked together, the secret image is revealed without the requirement of any computation whereas the conventional approaches to visual cryptography suffers from inefficiency in terms of number of bits of secret conveyed per bit of shares.
Recursive hiding of secrets with applications to the images increases the efficiency of visual cryptography which makes it possible to incorporate additional secret information that serves as a steganographic channel. The idea involved is recursive hiding of smaller secrets in shares of larger secrets with secret sizes doubling at every step, thereby increasing the information that every bit of share conveys to (n-1) / n bit of secret i.e. nearly 100%.
The proposed methodology initiates with the each pixel values of the original image represented as a single bit. For images with three or more gray levels, each pixel must correspond to a string of multiple bits with combination of 0's and 1's. The procedure of pixel reversal for each pixel value. The value obtained from the reversed value is taken as difference from a first random number generated. Therefore, if *m* pixels share a pixel of the original image *(k,n)* in a –n reversal method, then a grayscale –n reversal needs at *m(g-1)*least pixels to share a pixel of a grayscale image where *g* is the number of binary string. The procedure is repeated for the same values again and stored as the matrix named Share 1.

The difference between the first random number and newly generated second random number is obtained followed by the pixel reversal technique as done previously and stored in a matrix named Share 2.

In the reconstruction phase, any *k(k-1)* participants can reconstruct the grayscale image with optimal contrast by performing a sequence of stacking and reversing operations on their transparencies. The reconstruction of the grayscale image is done by performing XOR operations of the two shares Share1 and Share 2.

The Sigmoid function is performed on each pixel value for the image enhancement. The enhancement approach is a point process performed directly on each pixel of an image independent of all other pixels in that image to change the dynamic range.

A mask is passed over image pixel by pixel starting from image's upper right corner. Each pixel intensity value obtained so far from the above steps is equal to its added intensity value of this mask with the original image.

$O(i,j) = I(i,j) + I(i,j) * c * \frac{1}{1+e^{-1(i,j)}}$,

Where, $O(i,j)$ is the output image

$I(i,j)$ is the unprocessed input image

C is a factor

The value of c is dependent on the enhancement process which can be user specified value ranging from 0 – 255.

In proposed approach, when the partitions of white pixel are stacked upon each other one third of the pixel is white and hence appears light gray to human eye. However, the subpixels of the black pixel are so arranged that when 2 shares are stacked together, the resulting pixel is completely dark. Another way to create subpixels would be to have only one third of the subpixel colored dark. Therefore, when subpixels of a larger white pixel are stacked upon each other they would appear light gray and the stacking of the subpixels of a black pixel would result in dark gray. However, the human eye can perceives the difference between gray and completely dark pixels better than two different shades of gray itself.

THE PROPOSED ALGORITHM

Input: Secret Gray scale image (SI)

Output: Valid Shares Share1, Share2

Method:

Step1:- Pixel Sij with position i and j is the input called original pixel.

Step2:- Apply pixel reversal i.e Sij´ = 255 – Sij .

Step3:- Use pseudo - random number generator (0.1 to 0.9) to reduce Si j´ randomly.

Step4:- Take the difference of Sij´ with original pixel Sij.

Step5:- Use pseudo-random number generator to reduce reversed value of Sij´ randomly.

Step6:- Apply pixel reversal i.e Sij´´ = 255 – Sij´

Step7:- Store in matrix as image called share 1.

Step8:- Take the difference of two random number generators with original pixel S ij .

Step9:- Apply pixel reversal i.e Sij´´´ = 255 - Sij´.

Step10:- Store Sij´´´ in matrix as **image** called share 2.

Step 11:- Stack both the share 1 and share 2

Step 12:- Apply the sigmoid mask to each pixel

Step 13:- Display the final encrypted image.

EXPECTED OUTCOMES:

Our proposed methodology tries to overcome the drawback of the existing approach by applying sigmoid function in spatial domain for contrast improvement in the resulting secret image which possesses a much higher readability and proves highly effective in dealing with poor contrast images. This approach tries to enhance the details in images without affecting the details or increasing any amount of noise present to the output image.

CONCLUSIONS:

Visual Cryptography provides one of the secure ways to transfer images on the Internet. The advantage of visual cryptography is that it exploits human eyes to decrypt secret images with no computation required. Our proposed methodology tries to overcome the drawback of the existing approach by applying sigmoid function in spatial domain for contrast improvement in the resulting secret image. The resulting image possesses a much higher readability and proves highly effective in dealing with poor contrast images. This approach enhances details in images without affecting the details or increasing any amount of noise present to the output image.

FUTURE WORK:

The proposed algorithm in this thesis work produces better results for visual cryptography which helps in security of the data. The procedure involves encrypting individual shares of image which divulge the information about the original secret image. Moreover these images can be secretly transmitted or distributed over an entrusted communication channel. In the coming days, such a simple approach can be applied in a video visual cryptography for analyzing the spatio-temporal images.

REFERENCE:

[1] Naor, M. and Shamir, A., Visual cryptography, In Proc. Eurocrypt 94, Perugia, Italy, May 9–12, LNCS 950, Springer Verlag., 1994, pp. 1–12.

[2] V. Rijmen, B. Preneel, Efficient colour visual encryption for shared colors of Benetton, Eurocrypto'96, Rump Session, Berlin, 1996.

[3] C.C. Chang, C.S. Tsai, T.S. Chen, A technique for sharing a secret color image, Proceedings of the Ninth National Conference on Information Security, Taichung, May 1999, pp. LXIII–LXXII.

[4] Y.C. Hou, F. Lin, C.Y. Chang, Improvement and implementation of the secret color image sharing technique, Proceedings of the Fifth Conference on Information Management, Taipei, November 1999, pp. 592–597.

[5] Y.C. Hou, F. Lin, C.Y. Chang, A new approach on 256 color secret image sharing technique, MIS Review, No.9, December 1999, pp. 89–105.

[6] Y.C. Hou, C.Y. Chang, F. Lin, Visual cryptography for color images based on color decomposition, Proceedings of the Fifth Conference on Information Management, Taipei, November 1999, pp. 584–591.

[7] Hiroki Koga and Hirosuke Yamamoto, Proposal of a lattice-based visual secret sharing scheme for color and gray-scale images. IEICE Transaction on Fundamentals, E81- A(6):1262– 1269.

[8] Haibo Zhang, Xiaofei Wang, Wanhua Cao and Youpeng Huang, "Visual Cryptography for General Access Structure Using Pixel-block Aware Encoding", JOURNAL OF COMPUTERS, VOL. 3, NO. 12, DECEMBER 2008.